Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A system of digital data encryption in a digital device, comprising:

an integrated encryption key generator generating ~~at least one key~~ **a plurality of keys** based on input received from an inaccurate timing source **each time the digital device is reset**;

a data buffer;

an input/output register that interfaces with memory of the digital device;

a control pad coupled to the input/output register; and

a memory controller that directs digital data from the memory to the data buffer with the digital data passing through the encryption key generator prior to entering the input/output register, wherein the integrated encryption key generator is coupled between the data buffer and the input/output register, and the integrated encryption key generator, the data buffer, the input/output register, the control pad and the memory controller are formed on a single substrate and are accessed through the control pad.

2. (Previously presented) The system of claim 1, where the encryption key generator includes:

an inaccurate clock;

a key store; and

a linear feedback shift register that generates a pseudorandom bit pattern while the linear feedback shift register is enabled and stores a plurality of bits as at least one key in the key store.

3. (Previously presented) The system of claim 2, where the encryption key generator further includes a random number generator that receives the pseudorandom bit pattern from the linear feedback shift register and provides a random number for use by the digital device.

4. (Currently amended) The system of claim 2, where the encryption key generator further includes:

a pseudorandom bit pattern generator that creates a bit stream; and

a key store that stores portions of the pseudorandom bit pattern as ~~**the at least one key**~~ **at least one of the plurality of keys**.

5. (Previously presented) The system of claim 4, including a pseudorandom number generator that selects a portion of the pseudorandom bit pattern to be a random number.

6. (Cancelled)

7. (Previously presented) The system of claim 2, including:

a sub-key generator that creates a sub-key based on data from the memory controller and a selected key from the key store; and

a combiner that combines the sub-key with the digital data.

8. (Previously presented) The system of claim 7, further including a data mixer that mixes bits of a byte of the digital data prior to the byte being combined with the sub-key.

9. (Currently amended) A system configured to decrypt encrypted digital data stored in memory of a digital device, comprising:

an encryption key generator receiving a signal from an inaccurate clock and generating a plurality of keys for encrypting the encrypted digital data **when the encryption key generator is reset**;

a memory controller that generates a memory request to retrieve the encrypted digital data; and

an encryption circuit that decrypts the encrypted digital data in response to the memory request of the memory controller using one or more of the plurality of keys.

10. (Previously presented) The system of claim 9, including a combiner that combines one of the plurality of keys with bank and row information contained in the memory request resulting in a sub-key.

11. (Original) The system of claim 10, including a data mixer that unmixes bits within a byte after the sub-key is applied to the encrypted digital data.

12. (Currently amended) A method of digital data encryption in a digital device, comprising:

generating a plurality of keys based on input received from an inaccurate clock **when the digital device is cycled**;

storing the plurality of keys;

placing the digital data in a data buffer; and

encrypting the digital data using the at least one of the plurality of keys while the digital data is being placed in a rewritable memory.

13. (Previously presented) The method of claim 12, where the generating the plurality of keys includes:

generating an inaccurate clock signal;

creating a pseudorandom bit pattern; and

storing at least one portion of the pseudorandom bit pattern in a key store as the plurality of keys.

14. (Previously presented) The method of claim 13, where the pseudorandom bit pattern is generated by a linear feedback shift register.

15. (Previously presented) The method of claim 13, further including generating a random number from the pseudorandom bit pattern.

16. (Cancelled)

17. (Previously presented) The method of claim 15, further including selecting a portion of the pseudorandom bit pattern to be used as a random number.

18. (Previously presented) The method of claim 12, further including:
mixing bits of a byte of the digital data with a data mixer; and
combining the byte with one of the plurality of keys.

19. (Previously presented) The method of claim 12, further including:
generating a sub-key with data from the memory controller and the key; and
combining the sub-key with the digital data.

20. (Previously presented) The method of claim 19, further including:
mixing bits of a byte of digital data with a data mixer; and
combining the byte with the sub-key.

21. (Previously presented) The method of claim 13, further including generating a random number from the pseudorandom bit pattern.

22. (Currently amended) A method to decrypt encrypted digital data stored in memory of a digital device, comprising:
generating a plurality of keys based on input received from an inaccurate clock **when the digital device is cycled**;
generating a memory request to retrieve the encrypted digital data; and
decrypting the encrypted digital data using one of the plurality of keys.

23. (Previously presented) The method of claim 22, further including combining one of the plurality of keys with bank and row information contained in the memory request to generate a sub-key.

24. (Previously presented) The method of claim 23, further including unmixing a byte of encrypted digital data with a data mixer.

25. (Currently amended) A set-top box apparatus in receipt of digital data for storage in a rewritable memory, comprising:

an encryption circuit ~~**with at least one key**~~ **generating a plurality of keys when the encryption circuit is reset**;

a data buffer filled with the digital data; and

a memory controller that directs the storage of the digital data in the rewritable memory with the digital data being encrypted by the encryption circuit and the at least one key after the digital data has entered the data buffer but prior to being stored in the rewritable memory.

26. (Original) The set-top box apparatus of claim 25, where the encryption circuit further includes:

a pseudorandom bit stream generator that creates a pseudorandom bit stream; and

a key store that stores the at least one key that is selected from the pseudorandom bit stream.

27. (Previously presented) The set-top box apparatus of claim 25, where the encryption circuit further includes:

a data mixer that mixes bits of a byte of the digital data; and

a combiner that combines the byte with the at least one key.

28. (Previously presented) The system of claim 1 wherein the memory controller that directs digital data from the memory to the data buffer with the digital data passing through the encryption key generator prior to entering the input/output register comprises means for encrypting the digital data prior to entering the input/output register.

Claim 29 (cancelled).